

Statement of Dr. G. Pete Nanos

Director

Los Alamos National Laboratory

Submitted to:

United States House of Representatives

Committee on Energy and Commerce

Subcommittee on Oversight and Investigations

March 18, 2005

Introduction

Mr. Chairman and members of the Committee, thank you for the opportunity to discuss the security program at Los Alamos National Laboratory. My name is Dr. Pete Nanos and I have served as Director of the Department of Energy's Los Alamos National Laboratory since 2003. I came to the Laboratory from the Navy where I retired as a Vice Admiral.

To begin, I want to emphatically state that the employees of Los Alamos National Laboratory are dedicated to the national security mission of this great nation and they take very seriously their responsibilities to personally safeguard America's secrets. Our contributions to the safety and security of the American people are significant, and we continue to serve on the front lines of the effort to build and sustain our collective defense. Clearly a component of that mission is the need to safeguard the national security information entrusted to our care. I am here today to tell you that I believe we are a better Laboratory today as it relates to security, and I want to reaffirm to you our commitment to be even better.

I have spent considerable time since assuming leadership of the Laboratory evaluating our strengths and weaknesses and working with the University of California to improve the overall direction of the Laboratory. As you know, I suspended Laboratory operations last summer. This was not an easy decision. I would like to spend some time here explaining what led to the suspension of operations. At the outset, it is important to note that during the suspension of operations, the Laboratory was open and employees were required to come to work throughout the entire suspension. During this period, employees

did productive work related to safety and security, in support of our mission. I will get into additional detail on this later in my testimony.

Let me emphasize that at no time did we suspend activities that were immediately critical to national security and or the continuity of operations, security and environmental compliance and protection.

Many of you are familiar with the two major incidents that led to my decision to suspend operations: the July Classified Removable Electronic Media (CREM) incident, which I will describe further below, as well as a safety incident just days later where a Lab student's retina was burned by a laser due to faulty safety practices. What many people do not know is that these two incidents alone did not lead to my decision. I would like to provide some additional context, and start by noting that my decision was made in close consultation with the University of California, the Department of Energy and the National Nuclear Security Administration. Prior to these incidents, my management team and I were tracking a recent rise in safety and security incidents. In addition, we were noting correlations in performance in the areas of safety, security, and compliance. Those employees who performed poorly appeared to do so in all of these areas. The other major factor that concerned me with the July CREM incident is that it showed clear signs of a behavior problem. This was in sharp contrast to earlier incidents where it was clear that for the most part good people who were trying to do the right thing had made honest mistakes. Given this backdrop, when I was confronted with back-to-back examples of seeming disregard for basic safety and security rules, I had serious concerns regarding the

security and safety of Laboratory operations and therefore, in good conscience, had no choice but to suspend all operations at the Laboratory.

During the suspension of Laboratory operations, and the subsequent restart, we learned that there were many good reasons to take the actions we did. In partnership with DOE and NNSA, we followed a rigorous and strategic process, dividing the entire Laboratory into risk levels:

- Risk Level 1, the lowest level, which is general office work;
- Risk Level 2, medium risk, which represents moderate-hazard work such as construction; and
- Risk Level 3, high risk, which includes our high-hazard programmatic work involving CREM and special nuclear materials (SNM).

We conducted Management Self Assessments of all of our operations, and all of our Level 2 and 3 operations had to present their findings to a Resumption Review Board (RRB), which was made up of personnel from the Laboratory, the National Nuclear Security Administration's Los Alamos Site Office, as well as the DOE Office of Assessment who observed and assisted in all aspects of the review. For Level 3 work, an additional internal review was conducted by a Laboratory Readiness Review (LRR) panel, prior to approval by myself, and ultimately resumption. The LRR consisted of Laboratory personnel who were from outside of the organization being reviewed. The NNSA site office in Los Alamos worked very closely with us on all aspects of the restart. We resumed operations as quickly as possible, with 100% of our Level 1 work up and

running on August 18, 2004, one month after the suspension of operations began, and the majority of operations up and running by late September/early October. Some of our highest-hazard operations did not resume until February 2005. It is important to note that 89% of the Laboratory's activities were classified as Risk Level 1.

What we found in our assessments validated our decision to suspend Laboratory operations. We identified more than 3,000 issues (ranging from safety compliance issues to permitting violations) that need to be addressed, including 350 "pre-start" issues that we felt had to be addressed before an activity could restart. We fixed the 350 pre-starts and have created an Operational Efficiency Project to implement the remaining fixes and changes over the coming years.

Below, I'd like to spend a few minutes covering the July 2004 incident, and more importantly, what we have done to correct the shortcomings that allowed the incident to occur.

The Accountable CREM Incident

First, and perhaps most importantly, we know with high confidence that the disks never existed. Rather, what we had was an issue of barcode labels entered into our accountability system but never affixed to actual media, which was compounded by the falsification of an inventory sheet by two employees indicating that the disks did exist. This conclusion is supported by independent investigations completed by the DOE and

the FBI. Given the identification of the most likely cause, we are left with the questions – why did it happen and how did we get ourselves into this situation?

Our analysis of the incident led us to the following conclusions regarding the direct causes:

- The direct cause of this incident was placing unattached barcodes into accountability (an unauthorized practice) without confirming their actual use. Simply put, the classified matter custodian issued the barcodes and entered them immediately into the accountability database. Unfortunately, the employee who received the barcodes failed to realize that the barcodes were accountable and should be tracked. The employees subsequently destroyed them without reconciling the discrepancy with the custodian.
- We also missed the opportunity to discover and reconcile the problem in an annual inventory of accountable classified matter conducted in April 2004. This inventory failed to identify the “missing” barcodes because the custodians did not properly complete the inventory and subsequently falsified the inventory records. In addition, line managers responsible for the operation failed to ensure the inventory was properly conducted and subsequently verified that the inventory was complete and accurate, and that all items were accounted for. That was clearly not the case.

In the process of conducting the root cause analysis of the incident we reached the conclusion that while human error and improper action were the direct causes, there were

additional systemic weaknesses that contributed to this incident, and that would allow similar incidents to occur again:

- The sheer size and geographic spread of accountable CREM operations increased the likelihood of an incident.
 - The inventory of accountable CREM exceeded 80,000 pieces at its high point.
 - There were over 4,500 employees with daily direct access to the media.
 - Our classified operations are widely dispersed, spread over 40 square miles.
 - The transaction volume is large, with daily movement of classified items between organizations within LANL and throughout the DOE Complex.
- The lack of detailed supporting documents (e.g. checklists and plans) to serve as job aids for employees engaged in classified work activities hindered effective performance.
- Custodians responsible for safeguarding and controlling classified items suffered from a variety of organizational ailments, including:
 - Lower job status
 - Lack of authority
 - Part-time job for many
 - Lack of training specific to CREM handling and control
 - Lack of support/conflict of interest within their parent organizations
- The absence of a DOE or LANL standard accountability system increased the potential for classified items to “drop through the cracks” as they moved between organizations. In March 2004 this problem was recognized, and with the concurrence

of the University of California, the Laboratory is implementing a single site-wide accountability system.

The Response to the Accountable CREM Incident – Holding People Accountable

In light of what we learned during our inquiry it was necessary to take very drastic steps, both in terms of holding people accountable for their actions and in changing the classified control program to help prevent a recurrence of the incident.

In terms of personnel actions, three employees had their employment terminated as a result of their involvement in this incident. Four employees received written reprimands and suspension without pay, including the Division leader who was also removed and reassigned to non-supervisory duties. All seven employees received administrative sanctions in the form of security infractions, which are permanently filed in their personnel security records and factor into the DOE's decision process for granting continued access to classified information. The infractions were issued for causes including:

- Failure to properly conduct classified media inventories and falsification of records;
- Failure to reconcile accountable CREM with inventory records; and
- Management failure to provide adequate oversight.

The NNSA also exercised its right to hold the University accountable for the incident. LANL received an “unsatisfactory” performance rating in the “operations” area of the annual performance assessment. As a result, in January, 2005, NNSA withheld 67% of

UC management fee, with a penalty assessment of \$5.8M out of a possible \$8.7M performance fee pool. This represents the largest DOE-directed management fee cut in history.

The Response to the Accountable CREM Incident – Changing the Classified Control System

It is safe to say that we have learned a great deal from this recent incident. After holding people accountable for their actions, we turned our attention to completely revamping the classified control system to help prevent a recurrence of this incident. With the concurrence of the University of California, LANL acted to move all media into secure centralized libraries, to establish full-time custodians and fund expanded classified media-less computing. The major elements of our efforts include the following:

- All accountable CREM has been moved into one of 20 centralized “base” libraries. Fourteen “satellite” libraries have also been established to provide as-needed secure storage of media in close proximity to operational work areas. These “satellites” are each associated with a “base” library and are under the strict control of the “base” library custodians. The new configuration represents a significant reduction in the number of CREM storage locations across the Laboratory. Where previously CREM was stored in 89 buildings with 733 rooms, the new CREM libraries are housed in 29 buildings with 37 rooms. This represents a 95% reduction in the number of rooms.
- Each library was put through a rigorous inspection and certification process prior to commencing operations.

- Trained and certified Classified Library Custodians are assigned to each library – they are responsible for checking items out and conducting daily transactional inventories to ensure classified media is positively accounted for at all times.
- The library custodians are deployed security professionals reporting directly to the Security Division.
- To ensure the libraries maintain a high level of performance we began no-notice inventory inspections.
- To solve the issue of fragmented accounting systems we have begun the procurement of a Lab-wide inventory/accountability system.
- We are pushing hard on line organizations to destroy unneeded accountable CREM, we have destroyed over 7,000 items in the past two months, with many more entering the destruction pipeline. As of March 4, 2005, the Laboratory has 20,074 pieces of CREM.
- To help further reduce the accountable CREM holdings we are continuing our effort to replace stand-alone classified computers with “media-less” computer networks.
- LANL is rapidly driving towards the goal of having less than 2,000 pieces of accountable CREM. We believe this number reflects the long-term static inventory and once achieved will represent more than a 97% reduction in accountable CREM holdings. With continued investments in “media-less” networks, we hope to hit this goal by the end of FY06.

I believe it also very important to point out that many of the problems we have had in the past regarding difficulties with safeguarding classified information can be tied to two

over-arching issues. The first is the failure to invest in what I would term “engineered” solutions. In many cases we have had good employees trying to do a difficult job without the benefit of the right tools. The best example is the shortage of classified networks that do not rely on high-risk portable CREM – simply put, the more we invest in classified networks the more we reduce the likelihood of losing control of classified information. It is important to note that technology enhancements alone will not solve the entire problem. Along with engineered solutions we are ensuring that strong management oversight is in place to detect problems and solve them before they become a crisis. Thanks to funding support from Congress, we are moving to finish our expansion of media-less computing systems. This support is paving the way for continued improvements in our security infrastructure and will position us to more effectively meet our security challenges.

The second over-arching issue is that we have not done as much as we could to provide our scientists and engineers with the necessary security resources. As with any large operation involving highly classified information, the rules and requirements for security can be difficult to understand and implement. We are deploying security experts to our line organizations for the sole purpose of helping them to continue to build solid security programs. Our security experts are focusing on building better security plans, providing real-time training, and wading through the security rules to find the right solutions to adapt to our operations. The feedback I’m receiving is that this model is a resounding success – we will continue to put a great deal of effort into building this partnership and

we have high hopes for its ability to substantially improve security performance across the Laboratory.

How These Changes Are Improving Our Operations

While we are continuing to make enhancements to the new model for controlling accountable classified media, initial indications reveal that the system is working well, with tangible benefits for both improved security control as well as operational efficiencies resulting from the economies of scale we are seeing in the library approach. The major benefits include:

- Substantial improvement in daily control and accountability for CREM – it is under the direct ownership of approximately 40 custodians. This represents a more than 99% reduction from the approximately 4,500 employees who previously had direct access.
- Clear requirements and training for handling accountable CREM when it is checked-out of the library – a rigorous training process is required before you can be assigned as a “borrower” of the media.
- Line organization managers and staff are now able to concentrate on their mission – they are still responsible for protecting the media when it is checked out, but they do not have to spend countless hours maintaining individual accountability and control systems.

Apart from the very tangible benefits we are seeing from our efforts to change the security model, we are also starting to see the intangible benefits tied to attitudes and

perceptions of the workforce. As a result of the incidents we have had over the past several years there was a real concern among our employees that the task of doing their job safely and securely was getting increasingly difficult, with the addition of more and more policies and procedures to follow. With each new set of policies and procedures came the perception of increased risk in inadvertently violating the rules. I am particularly proud of the fact that instead of making the job even more difficult to do, our response to this most recent incident has actually simplified the work and clarified the responsibilities our workers have in protecting classified information. As a result of this simplification our workforce is becoming increasingly confident in taking personal responsibility for safety and security – as with any human endeavor, personal responsibility is the linchpin of performance. I’m confident that we are rebuilding the sense of trust and mutual support that is absolutely essential to sustaining our operations and delivering on our national security mission.

Physical Security Initiatives

Finally, I want to take this opportunity to tell you what we are doing on upgrading the physical security of the Laboratory to deal with the post-9/11 world. As you know DOE has recently revised their Design Basis Threat (DBT), which articulates the adversary force size and capabilities that we must be able to defend against. I will tell you quite honestly that this new DBT represents a significant challenge to nuclear sites, but it is a challenge we must meet. We have been working literally from September 11, 2001, to fundamentally change the security posture for our site. An amazing array of upgrades and improvements has been made – all for the singular goal of safeguarding the people and

security interests under our control. I am particularly proud to point out that the most recent DOE inspection of the protective force performance at TA-18 clearly shows that the facility is well defended and the nuclear materials housed there are secured. The Department has made the decision to relocate the TA-18 mission and the nuclear materials to Nevada and we are fully committed to making this happen as quickly as possible.

To address the recently revised DBT we are developing a comprehensive project plan designed to guide our long-term strategy for meeting the new challenges. The project plan, which is due to NNSA in July of this year, includes new initiatives to control access to the site, upgrades in the size and lethality of our protective force, consolidation of nuclear operations to achieve economies of scale for our protection operations, and new construction of barriers and alarms at key facilities. I am confident in our ability to defend the site, and that confidence is anchored by DOE assessments that tell us we are good and getting better. We will continue to spare no effort in our quest to ensure the security of Los Alamos and the national security mission with which we are charged.

Summary

As I mentioned in my opening comments, the decision to suspend Laboratory operations was not an easy one. The decision has caused great turmoil within the Laboratory and generated a fair amount of second guessing. From my vantage point the suspension of Laboratory operations was absolutely the right thing to do – the pain we have experienced is more than offset by the long-term gain we will see from this investment.

Today we have a solid grasp on safety and security risk areas within the Laboratory based on comprehensive risk analyses. As a result, we are better situated to understand the safety and security implications of the work we do. The suspension of operations has introduced a formality of operations to an institution that desperately needed it. I cannot sit here today and tell you that we will never have another safety or security incident at Los Alamos; our operations are too large and too complex to ever be able to give you a 100% guarantee. But what I can guarantee is that the management at the Laboratory and the University of California is committed to continuing its improvements to both safety and security. We will take an outstanding operation and make it even better, and we will continue to deliver on our commitment to the safety and security of this nation, I promise you that.

Again, thank you for allowing me the opportunity to address you and I would be glad to answer any questions you may have for me.